Cybersécurité

Les bonnes pratiques à transmettre à votre équipe pour éviter le pire

Sommaire

Introduction

La transformation digitale (grandement accélérée par la COVID-19) et l'explosion des modes de travail hybrides suscitent des inquiétudes légitimes quant à la capacité des organisations à gérer le risque cyber. Cette menace omniprésente et insidieuse peut briser une entreprise. Les attaques augmentent chaque jour et personne n'est à l'abri.

Au-delà des solutions technologiques développées pour défendre et combattre les risques, nous pouvons accomplir encore plus grâce à une meilleure formation, une meilleure sensibilisation et une meilleure connaissance du comportement humain.

Des études le confirment : de nombreuses violations cyber sont le résultat de vulnérabilités humaines et non d'une défaillance technologique.

La cybersécurité est désormais un sujet que tout le monde doit prendre en compte, que ce soit dans sa vie personnelle ou professionnelle. Mais, pour quelles raisons ?

1. Les plateformes en ligne sont des cibles plus importantes que jamais étant donné l'étendue et la criticité des éléments qu'elles contrôlent.
2. La quantité et la valeur des données que nous produisons et stockons ont augmenté de manière exponentielle. Ces données sont une mine d'or pour le cyber criminel.
3. L'interconnexion du monde permet à un plus grand nombre de personnes - quelle que soit leur situation géographique - de créer des situations dangereuses plus facilement.
4. Les attaques sont de plus en plus sophistiquées, les attaquants sont mieux organisés, mieux financés et plus difficiles à traduire en justice.

Ce guide a pour but d'aider les leaders qui sont conscients de l'omniprésence du risque cyber et de leur proposer des conseils et bonnes pratiques à transmettre à leurs équipes (souvent moins averties) afin d'atténuer les effets néfastes qu'une cyberattaque pourrait engendrer.

La cybersécurité expliquée à votre équipe

La cybersécurité désigne le processus et la pratique cyclique de sécurisation des données, des réseaux et des ordinateurs contre toute utilisation abusive, que ce soit par des cyberattaques externes ou d'autres menaces.

Les organisations ont pour obligation (RGPD) de **protéger les données personnelles** :

- Coordonnées,
- Mots de passe,
- Numéros de carte de crédit,
- Renseignements sur les comptes bancaires,
- Numéros de passeport et de permis de conduire,
- Numéros de sécurité sociale,
- Dossiers médicaux,
- ...

mais aussi les **données sensibles ou confidentielles sur certains projets** :

- Réorganisations,
- Plan stratégique,
- Lancement majeur,
- Résultats,
- R&D,
- Acquisitions,
- ...

Quelques chiffres pour une prise de conscience immédiate

978 millions
de personnes sont concernées par une cyberattaque chaque année. (source)

90%
des brèches de cybersécurité sont dues à une erreur humaine. (source)

En matière de protection des données,
73% des Français
ne font pas confiance aux logiciels chinois
et 49%
ne font pas confiance aux logiciels US. (source)

Le phising
est le mode d'attaque le plus fréquent. (source)

Les entreprises françaises identifient les incidents cyber comme
le risque n°1
au sein de l'organisation. (source)

La cybercriminalité coûte à l'économie mondiale
1 000 milliards
de dollars. (source)

Il faut en moyenne
197 jours
pour une entreprise avant de découvrir qu'elle a été victime d'une fuite de données. (source)

En France,
8 entreprises sur 10
sont touchées par des cyber attaques chaque année. (source)

En France, le coût moyen d'un cyber-incident est
de 35 000 euros. (source)

---

1 entreprise française sur 2
se dit inquiète quant à sa capacité à faire face aux cyber-risques. (source)

Les failles de cybersécurité et les inégalités digitales sont
les 2 premières menaces
technologiques mondiales à court terme (0-2 ans) (source)

10 conseils pour les sensibiliser

La première étape pour améliorer la sécurité au sein de votre organisation est de sensibiliser les employés. Ils sont à la fois votre meilleur atour et votre plus grande menace en matière de sécurité.

Faire de la cybersécurité une priorité absolue pour les employés n'est pas une mince affaire quand on sait qu'ils ont eux aussi leurs propres missions et échéances.

Les conseils ci-dessous vous aideront à former, informer et sensibiliser vos employés au rôle qu'ils jouent dans la cybersécurité de votre organisation.

Montrez-leur ce qu'ils y gagnent

Une grande partie de ce que les employés apprennent pendant une sensibilisation sur la sécurité au travail peut être appliquée à la sécurité de leur compte personnel. Montrez-leur la valeur de l'information et ce qui concerne sa sûreté et sa sécurité sans vous focaliser uniquement sur les intérêts de l'entreprise.

Démontrez clairement que personne n'est à l'abri d'une attaque

Il ne s'agit pas de savoir *si*, mais *quand* une attaque va se produire. Il s'agit d'aider les équipes à réagir rapidement et efficacement pour bloquer l'attaque ou minimiser les dégâts.

Intégrez la sensibilisation à la sécurité dans votre processus d'accueil des nouveaux collaborateurs

Il n'est jamais trop tôt pour prendre de bonnes habitudes. Il est très logique d'intégrer la cybersécurité dans le processus d'intégration, car les nouveaux employés ont probablement accès à des comptes, à des mots de passe et à des informations sur les processus de l'entreprise.

Créez un plan officiel de formation à la cybersécurité

Pour aller avec le conseil ci-dessus, il devrait y avoir pour les employés un plan de formation, mis à jour régulièrement et facilement accessible. Faites appel à des experts et formateurs en cybersécurité. Ces professionnels peuvent mobiliser les employés et leur présenter les éléments de base et les particularités qu'ils devraient connaître pour leur travail.

Renseignez-les sur les politiques de confidentialité des données

Enseignez aux employés que l'utilisation de certaines données peut être restreinte même si elles sont disponibles. Par exemple, la plupart des entreprises tiennent à jour des listes de contacts qui ont choisi de ne plus recevoir des e-mails de leur part (liste opt-out). Les personnes qui leur envoient des e-mails violent cette politique.

Effectuez des simulations de crise

Ces situations de crise peuvent être mises en place par votre équipe de sécurité interne ou par une source extérieure. Elles doivent être adaptées à des situations spécifiques et mettre l'accent sur les attaques que les employés pourraient subir afin qu'ils puissent apprendre et retenir des choses tout en s'améliorant.

Envoyez régulièrement des mises à jour

Le protocole, les menaces, les nouvelles escroqueries, les virus, les mises à jour logicielles et autres informations importantes sur la cybersécurité doivent être communiqués systématiquement.

Communiquez de façon claire et concise

Essayez d'éviter les longs e-mails et les notes de service. Beaucoup d'employés lisent les deux premières phrases avant de les supprimer. Essayez plutôt de créer des vidéos ou des infographies. Même si vos employés ne sont pas très intéressés par la sécurité, la lecture répétée de phrases et d'actions sous forme visuelle les aidera à se souvenir de ces messages lorsque quelque chose d'inhabituel surviendra.

Organisez régulièrement des formations sur la sécurité

Au fur et à mesure que de nouvelles menaces et de nouveaux modèles de menaces apparaissent, une formation régulière à la sécurité doit être mise en œuvre à l'échelle de l'entreprise, afin de s'assurer que les failles de sécurité qui permettent aux activités malveillantes de pénétrer l'entreprise ne sont pas exposées.

Intégrez la cybersécurité dans votre culture d'entreprise

Les dirigeants d'entreprise sont responsables de la culture de l'entreprise. Ceux qui prennent la cybersécurité au sérieux inciteront leurs employés à faire de même. Créez une culture favorable à la cybersécurité en désignant des leaders internes qui auront pour but de favoriser des pratiques exemplaires en matière de cybersécurité auprès des employés.

8 conseils à appliquer au travail

Verrouillez virtuellement et physiquement les appareils et les espaces de stockage

Assurez-vous de verrouiller votre appareil chaque fois que vous le laissez sans surveillance et assurez-vous également que les appareils et les services que vous utilisez se verrouillent automatiquement lorsqu'ils sont inactifs. Ceci s'applique également aux pièces ou aux lieux de stockage qui contiennent des informations ou des dispositifs sensibles.

Utilisez un gestionnaire de mots de passe

Les gestionnaires de mots de passe génèrent des mots de passe complexes uniques pour chaque site et service. N'utilisez pas le même mot de passe pour plusieurs sites et utilisez toujours un mélange unique de lettres majuscules et minuscules, chiffres et autres caractères. Plus de détails dans la section mot de passe de ce guide.

Utilisez l'authentification multifacteurs

Elle apporte des niveaux de sécurité supplémentaires et vous assure que les comptes importants ne sont pas facilement piratés si les mots de passe sont découverts.

Chiffrez les supports de stockage

Le chiffrement de données permet d'ajouter une couche supplémentaire de sécurité si jamais vos données sont compromises.

Sauvegardez souvent et régulièrement les données

Si le stockage des données est compromis, vous aurez les meilleures chances de conserver ces données si vous disposez d'une sauvegarde sécurisée.

Méfiez-vous des périphériques externes

Les disques durs, les clés USB et les smartphones peuvent infecter votre ordinateur lorsqu'ils sont branchés.

Ne partagez jamais d'informations sensibles avec un interlocuteur non autorisé

Cela peut sembler évident, mais trop souvent, les employés ressentent une certaine pression sociale quand quelqu'un d'autre leur demande des informations (cela s'applique également aux membres de votre organisation). En cas de doute, dites non et consultez un manager pour obtenir la permission. Ne donnez jamais votre mot de passe.

Ne sous-estimez pas l'intérêt des pirates informatiques pour votre entreprise

Les brèches et les attaques affectent les organisations de toutes tailles, y compris les jeunes entreprises et les TPE/PME. De nombreux outils de sécurité offensifs analysent sans discernement le Web à la recherche de vulnérabilités dans les services, l'accès à distance et les applications Web.

5 conseils pour leur sécurité en ligne

Utilisez un VPN (Virtual Private Network)

Il étend la protection de votre réseau au-delà de votre réseau privé lorsque vous n'êtes pas au bureau. Si quelqu'un est capable d'intercepter vos données en ligne, il ne lui restera que des données cryptées.

Soyez vigilants sur les transactions financières

Vérifiez toujours les transactions financières avec un manager, un RSSI ou un directeur financier avant de prendre toute mesure ou d'envoyer des fonds. Soyez prudent lorsque vous effectuez des opérations bancaires en ligne pour l'entreprise, n'utilisez que des appareils sécurisés autorisés par l'entreprise qui vous appartiennent et des réseaux WiFi sécurisés lorsque vous effectuez ces tâches.

Faites attention à ce que vous partagez sur les médias sociaux

Que vous soyez sur un compte personnel ou professionnel, les criminels peuvent obtenir des informations à partir de données sensibles que vous partagez et qui peuvent les aider à vous cibler.

Faites attention à vos e-mails (hameçonnage ou phishing)

Prenez le temps d'évaluer soigneusement les e-mails avant d'agir. Ne cliquez jamais sur les liens d'un expéditeur inconnu. Il peut se faire passer pour quelqu'un de votre entreprise ou d'une entreprise connue, utiliser une URL similaire à un site connu, utiliser des logos et des adresses e-mail déguisées. Portez une attention particulière aux détails (demande bizarre, fautes d'orthographes, etc). Tous les détails dans la section phishing de ce guide.

Ne travaillez que sur des réseaux et des périphériques sécurisés et fiables

Les WiFi gratuits ou publics peuvent être séduisants, mais ce sont des billets d'entrée faciles pour un hacker qui souhaite accéder à vos comptes et à vos informations. En cas d'usage d'un WiFi public, connectez-vous à votre VPN d'entreprise pour protéger votre accès.

2 types d'attaques fréquents et comment s'en prémunir

Le phishing

Dans cette approche, l'attaquant se fait passer pour un tiers de confiance (marque, banque, cadre de votre organisation, partenaire commercial) afin de manipuler le destinataire et l'amener à faire des actions qui mettent en péril ses données sensibles et/ou celles de son organisation. La plupart des attaques sont déployées par e-mail mais certains hackers exploitent désormais les réseaux sociaux, les applications de messagerie ou les SMS pour vous tromper.

La plupart des actions consistent à faire télécharger un logiciel malveillant (ex : rançongiciel) ou à faire remplir un formulaire sur un faux site web.

18 comportements qui doivent alerter vos équipes

Prenons l'exemple d'un e-mail et de tous les points sur lesquels nous recommandons d'être vigilant. La plupart des conseils sont aussi applicables pour un SMS ou un message sur les réseaux sociaux.

➤ **De : Manager@MaSociete.com (expéditeur)**

- L'e-mail de l'expéditeur semble différent de celui avec lequel mon interlocuteur communique habituellement.
- L'e-mail provient d'une personne extérieure à mon organisation et n'est pas lié à mes responsabilités professionnelles.
- L'e-mail a été envoyé par une personne au sein de mon organisation, un client, un fournisseur ou un partenaire et semble inhabituel ou hors sujet.
- L'e-mail de l'expéditeur provient d'un domaine suspect.

➤ **A : Moi@MaSociete.com (destinataire)**

- J'ai reçu un e-mail envoyé à une ou plusieurs personnes, mais je ne connais pas personnellement les autres personnes à qui il a été envoyé.

➤ **Date : Lundi 4 Septembre 2021, 03h30**

- L'e-mail a été envoyé hors des heures normales de bureau à un horaire inhabituel (ex : 2 heures du matin).

➤ **Objet :**

- L'objet de l'e-mail n'est pas pertinent ou ne correspond pas au contenu du message.
- L'e-mail est une réponse à quelque chose que je n'ai jamais demandé.

➤ **Contenu :**

- L'expéditeur me demande de cliquer sur un lien ou d'ouvrir une pièce jointe pour éviter une conséquence négative ou pour obtenir quelque chose de valeur.
- L'expéditeur me demande de communiquer des informations sensibles, personnelles ou confidentielles.
- L'e-mail sort de l'ordinaire ou comporte des fautes de grammaire ou d'orthographe.
- L'expéditeur me demande de cliquer sur un lien ou d'ouvrir une pièce jointe qui semble bizarre ou illogique.
- La demande de l'expéditeur d'ouvrir une pièce jointe ou de cliquer sur un lien me met mal à l'aise.

- L'expéditeur me demande de regarder une photo compromettante ou embarrassante de moi-même ou d'une personne que je connais.

➤ **Liens :**

- Au survol de ma souris sur le lien hypertexte qui est dans l'e-mail, l'adresse du lien qui s'affiche est celle d'un autre site web.
- J'ai reçu un courriel qui ne contient que de longs hyperliens sans aucune autre information, et le reste du courriel est complètement vide.
- L'e-mail contient un lien d'un site connu avec une faute d'orthographe. Exemple : www.banquedeluxernbourg.com ou le «m» est en fait constitué de deux caractères «r» et «n».

➤ **Pièces jointes :**

- L'expéditeur a inclus une pièce jointe que je n'attendais pas ou qui n'a aucun sens par rapport au message envoyé.
- Je vois une pièce jointe avec un type de fichier potentiellement dangereux ou dont je ne connais pas la terminaison.

Les mots de passe

Selon les recherches menées par le NordPass, la majorité des gens utilisent des mots de passe simples et faciles à retenir pour des raisons de praticités. Le problème est que la plupart des mots de passe mémorisables sont très vulnérables.

Top 20 des pires mots de passe utilisés en France en 2020

- 123456
- 123456789
- azerty
- 1234561
- qwerty
- marseille
- 000000
- 1234567891
- doudou
- 12345
- loulou
- 123
- password
- azertyuiop
- 12345678
- soleil
- chouchou
- 1234
- 1234567
- 123123

La liste complète est disponible **ici**.

Combien de temps faut-il à un hacker pour récupérer un mot de passe ?

Ce tableau présente la capacité d'un hacker à retrouver un mot de passe en fonction de sa complexité. Il est idéal pour faire prendre conscience à un public peu averti de la nécessité d'avoir un mot de passe plus complexe.

Nombre de caractères	Nombres uniquement	Lettres majuscules OU minuscules	Lettres majuscules ET minuscules	Nombres, lettres majuscules, lettres minuscules	Nombres, majuscules, minuscules et symboles
3	Immédiatement	Immédiatement	Immédiatement	Immédiatement	Immédiatement
4	Immédiatement	Immédiatement	Immédiatement	Immédiatement	Immédiatement
5	Immédiatement	Immédiatement	Immédiatement	3 sec	10 sec
6	Immédiatement	Immédiatement	8 sec	3 min	13 min
7	Immédiatement	Immédiatement	5 min	3 heures	17 heures
8	Immédiatement	13 min	3 heures	10 jours	57 jours
9	4 sec	6 heures	4 jours	1 an	12 ans
10	40 sec	6 jours	169 jours	106 ans	928 ans
11	6 min	169 jours	16 ans	6 000 ans	71 000 ans
12	1 heure	12 ans	600 ans	108 000 ans	5m d'années
13	11 heures	314 ans	21 000 ans	25m d'années	423m d'années
14	4 jours	8 000 ans	778 000 ans	1M d'années	5M d'années
15	46 jours	212 000 ans	28m d'années	97M d'années	2b d'années
16	1 an	512m d'années	1M d'années	6b d'années	193b d'années
17	12 ans	143m d'années	36M d'années	374b d'années	14B d'années
18	126 ans	3M d'années	1b d'années	23B d'années	1t d'années

Légende :
m = millions (1 000 000)
M = milliards (1 000 000 000)
b = billions (1 000 000 000 000)
B = billiards (1 000 000 000 000 000)
t = trillions (1 000 000 000 000 000 000)

source

NB : ce tableau date de 2012 et présente des résultats basés sur des attaques par force brute assez basiques. Avec les pratiques actuelles, le temps qu'il faut pour récupérer un mot de passe est largement réduit. La gendarmerie nationale propose une autre version ici et la société Cyberzen démontre qu'avec une attaque par dictionnaire, les résultats sont instantanés.

Anatomie d'un mot de passe fort

➤ Comprend plus de 12 caractères

Le nombre de caractères minimum conseillé varie selon les experts. Cependant, ils se rejoignent tous sur un point : plus un mot de passe est long, mieux c'est ! N'hésitez pas à aller au-delà des 12 caractères conseillés. Chez Wimi, nous recommandons 20 caractères aléatoires.

- **Comprend des chiffres, des symboles, des majuscules et des minuscules**

Utilisez un mélange de différents types de caractères pour rendre le mot de passe plus difficile à cracker.

- **N'est pas un mot de dictionnaire ou une combinaison de mots du dictionnaire**

Évitez les mots évidents du dictionnaire et les combinaisons de mots du dictionnaire. Tout mot en soi est mauvais. Toute combinaison de quelques mots, surtout s'ils sont évidents, est également mauvaise. Par exemple, « poisson » est un mauvais mot de passe, « poisson rouge » aussi.

- **Ne repose pas sur des substitutions évidentes**

N'utilisez pas non plus de substitutions courantes. Par exemple, il ne suffit pas de remplacer un « o » par un « 0 » pour rendre le mot de passe « p0isson » plus fort.

- **Ne comprend pas d'informations directement identifiables**

Évitez d'utiliser votre prénom, nom, numéro de téléphone, date de naissance, adresse et toutes autres informations personnelles qu'un hacker pourrait facilement retrouver sur le web.

- **Est unique**

Utiliser un seul mot de passe pour plusieurs comptes est le meilleur moyen de vous mettre en danger. La règle est simple : un mot de passe = un compte.

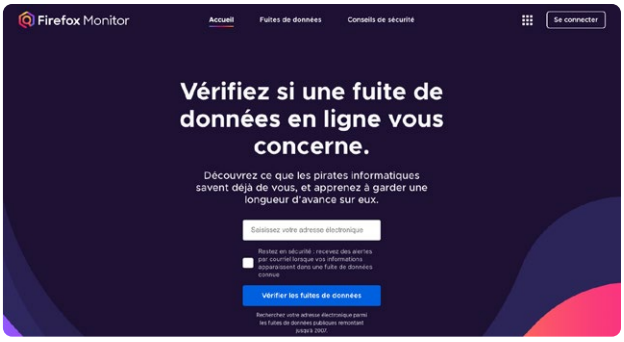
- **Est régulièrement renouvelé (dans certains cas)**

Prenez l'habitude de renouveler votre mot de passe tous les ans sur vos comptes clés (ex : ordinateur, boite mail, coffre-fort). Faites un changement dès que vous avez un doute sur la sécurité d'un compte ou lorsqu'un service que vous utilisez annonce s'être fait pirater.

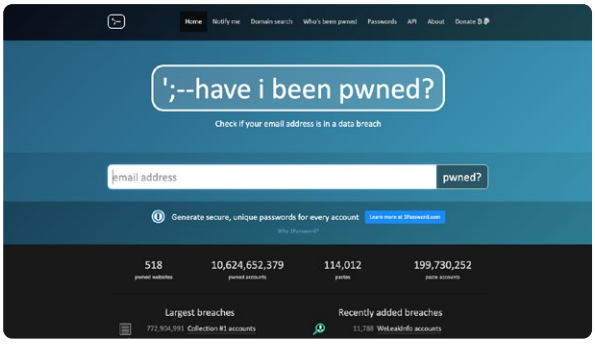
- **N'est jamais partagé**

Cela paraît évident mais votre mot de passe ne doit jamais être partagé avec qui que ce soit, ni être utilisé sur un appareil dont vous n'êtes pas le propriétaire.

Bonus : 2 outils pour savoir si une fuite de données en ligne concerne votre équipe :



https://monitor.firefox.com/



https://haveibeenpwned.com/

2 aspects techniques qui diminuent drastiquement les risques

Vos équipes testent de nouveaux outils et souhaitent en intégrer au sein de votre organisation. Invitez-les à inclure dans leurs recherches des solutions qui proposent l'authentification multi-facteurs et le chiffrement de bout-en-bout. En prenant en compte ces deux aspects, elles diminueront les effets néfastes d'une attaque cyber. Découvrons comment présenter ces deux points.

Authentification multifacteurs

L'authentification multifacteurs permet d'identifier un utilisateur en ligne en validant au moins 2 preuves fournies par celui-ci. Cette méthode d'authentification s'appuie généralement sur trois éléments :

1. Une information connue de l'utilisateur (un mot de passe, un code PIN) ;
2. Un objet qu'il possède (un smartphone, une tablette) ; et
3. Un élément unique, propre à sa personne (empreinte digitale, iris, visage, voix).

L'authentification multifacteurs repose sur l'idée qu'aucun facteur n'est parfait. Chaque facteur implémenté présente des points forts et des points faibles. Mais un deuxième ou un troisième facteur viendra compenser les limites du ou des autres, et inversement.

C'est pour cette raison que nous recommandons de privilégier des solutions en ligne qui vont au-delà de la demande d'un simple mot de passe en proposant ce type d'authentification.

Chiffrement de bout-en-bout

Le chiffrement de bout en bout est la méthode de chiffrement la plus sûre qui existe aujourd'hui.

Il s'agit d'un système qui protège le contenu de vos messages et de tous vos fichiers en les rendant illisibles à toute autre personne qui n'est pas le destinataire.

Vos données sont protégées contre le piratage ou le vol : même si une personne malveillante parvient à s'introduire dans votre système ou à voler l'un de vos appareils, vos données restent totalement illisibles. Vous avez le contrôle sur qui est autorisé à lire vos messages et vos fichiers.

Il est donc fortement conseillé de privilégier les outils et les logiciels qui proposent un chiffrement de bout-en-bout. Ils seront capables de protéger vos conversations, vos fichiers et toutes vos données contre les différentes menaces telles que la fuite et la falsification de données, le vol de mots de passe, d'ordinateurs ou de matériel d'hébergement ou l'intrusion.

Conclusion

Les ressources humaines sont l'atout le plus précieux d'une organisation. Elles constituent également la principale vulnérabilité en matière de cybersécurité. Grandes et petites entreprises, organisations gouvernementales, nul n'est épargné par ce constat.

Il est essentiel de s'assurer que les employés sont bien conscients des risques et des impacts des cybermenaces. Nous avons présenté de nombreux moyens pour réduire les chances qu'elles se produisent. Des habitudes saines et simples peuvent grandement contribuer à prévenir l'apparition de cyber-risques. De simples erreurs d'inattention (comme un clic sur un lien inconnu) peuvent causer la chute d'une entreprise.

La vulnérabilité d'une entreprise est directement influencée par la prise de conscience par ses employés des risques potentiels et leur capacité à mettre en place des actions préventives simples. Nous espérons que ce guide vous aidera à transmettre les bonnes pratiques.

Un dernier conseil pour la route : collaborez et demandez conseil à d'autres experts

Les organisations doivent adopter une attitude ouverte et partager les détails de ce qu'elles font en matière de cybersécurité. Les hackers passent toute la journée à attaquer les entreprises et toute la nuit à collaborer avec leurs pairs pour améliorer les prochaines attaques. Pourquoi les entreprises ne feraient pas la même chose pour mieux se défendre ?

Ressources utiles

Pour sensibiliser vos équipes, nous vous proposons d'aller au-delà de ce guide. Vous trouverez une courte sélection de TedTalks, séries, documentaires et sources sûres qui leur permettront de prendre un peu plus conscience des impacts de la cybersécurité.

Ted Talks

Cybersécurité : Faites votre choix en conscience – Yann Allain (Français)

Un point de vue sur les enjeux et les impacts de la cybersécurité pour les citoyens, les sociétés, les États. Bienvenue dans un monde où nous sommes dépassés par la réalité de l'(in)sécurité de nos infrastructures numériques…

The Humanity Behind Cybersecurity Attacks – Mark Burnette (Anglais)

Les entreprises dépensent des millions chaque année pour se protéger contre les cyberattaques. Cependant, la plupart des failles de sécurité ne sont pas dues à des attaques sophistiquées, mais à des défaillances humaines…

Your Human Firewall – The Answer to the Cyber Security Problem – Rob May (Anglais)

Les données personnelles sont une denrée précieuse, et nous en partageons trop. Rob introduit la notion de « pare-feu humain » pour se protéger dans un univers où une grande partie de notre vie se déroule en ligne.

Voici ce qui arrive quand on répond aux spams – James Veitch (Anglais sous-titres français)

Des e-mails suspects, des coffres sertis de diamants, des proches bloqués à l'étranger… Mais que se passe-t-il lorsqu'on y répond ? Suivez le récit de James qui a échangé des e-mails hilarants avec un spammeur.

Qu'est-ce qui cloche avec votre m0t de pa$$e ? - Lorrie Faith Cranor (Anglais sous-titres français)

Lorrie a étudié des milliers de vrais mots de passe pour comprendre les erreurs étonnantes et très courantes que les utilisateurs - et les sites sécurisés - commettent et qui compromettent la sécurité.

Les cinq lois de la cybersécurité – Nick Espinosa (Anglais sous-titres français)

Nick est expert en cybersécurité et en infrastructure de réseau connu comme un leader d'opinion et consulté pour ses conseils sur le futur de la technologie et la manière dont elle impacte les entreprises et les consommateurs.

Cybersecurity every day – Jaya Baloo (Anglais)

Jaya intervient fréquemment lors de conférences sur la sécurité, sur des sujets tels la surveillance de masse et la cryptographie. Dans cette vidéo, elle se plonge dans la cybersécurité et son impact sur notre vie quotidienne.

Séries

Mr Robot

L'histoire tourne autour d'Elliot, un talentueux hacker et ingénieur en cybersécurité qui souffre de troubles d'anxiété sociale. Sa vie bascule lorsque Mr. Robot l'invite à rejoindre un groupe d'hacktivistes pour détruire le plus grand conglomérat financier du monde. Toutes les scènes de piratage de la série sont très réalistes.

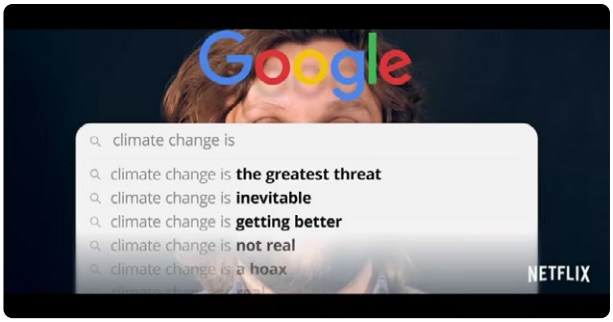
Black Mirror

Cette série dépeint le côté sombre de l'obsession de la société pour la technologie. Chaque épisode propose une histoire époustouflante montrant un futur dystopique où la technologie peut se retourner contre nous. Pour rendre les choses encore plus palpitantes, certaines des technologies présentées dans la série existent déjà.

Documentaires

The Great Hack

Ce documentaire expose les tenants et aboutissants de l'affaire Cambridge Analytica, société à l'origine du scandale sur la violation des données de millions d'utilisateurs sur Facebook. The Great Hack nous met face à la réalité de nos vies en ligne et nous fait réfléchir à deux fois avant de révéler nos données personnelles.



The Social Dilemma

Ce documentaire montre comment la plupart des réseaux sociaux construisent volontairement des fonctionnalités pour créer de la dépendance et s'immiscer dans notre vie privée. Vous verrez comment tout est pensé pour influencer nos actions et nous transformer en proies faciles pour les annonceurs et les propagandistes.

Pour ceux qui veulent plus de films et de séries autour de la cybersécurité, nous vous recommandons de suivre cette page.

Sources sûres en matière de cybersécurité

ANSSI | Agence nationale de la sécurité des systèmes d'information

Agence nationale de la sécurité des systèmes d'information (ANSSI)
https://www.ssi.gouv.fr/

CERT-FR | Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques

Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR)
https://www.cert.ssi.gouv.fr/

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Commission nationale de l'informatique et des libertés (CNIL)
https://www.cnil.fr/professionnel

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention du risque numérique (CyberMalveillance)
https://www.cybermalveillance.gouv.fr/

Wimi pour gérer vos projets sensibles et confidentiels

Vous recherchez un logiciel de travail collaboratif à la fois efficace, ergonomique et sûr ?

Wimi est une plateforme collaborative simple à utiliser et hautement sécurisée qui vous permet de collaborer efficacement sur tous vos projets sensibles tout en assurant une confidentialité absolue (chiffrement de bout en bout des données) et en vous protégeant des risques cyber.

Pour cela, le logiciel centralise et sécurise l'ensemble des données numériques échangées par l'équipe afin de mener à bien un projet (documents, tâches, appels vidéo/audio, calendriers projet, messages instantanés, etc.).

Wimi offre des fonctionnalités indispensables à l'efficacité des équipes ainsi qu'à la sécurité des données, telles que :

- un espace collaboratif associé à chaque projet ;
- une gestion centralisée des accès grâce à un système d'authentification renforcé ;
- un chiffrement de bout en bout des données ;
- une authentification multifacteurs ;
- une interface performante qui permet des gains de temps et une réduction des risques de contournements ;
- un contrôle et des alertes en cas de détection de flux et de comportements atypiques.

Autre atout majeur : vos données sont hébergées en France, par une société française indépendante en cours de qualification SecNumCloud auprès de l'ANSSI.